The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

02/19/2014

SUBJECT:

Vulnerability in Cisco Unified Computing System (UCS) Director Could Allow Remote Access

OVERVIEW:

A vulnerability in Cisco Unified Computing System (UCS) Director could allow an unauthenticated, remote attacker to take complete control of the affected device. The vulnerability is due to a default root user account created during installation. An attacker could exploit this vulnerability by accessing the server command-line interface (CLI) remotely using the default account credentials. An exploit could allow the attacker to log in with the default credentials, which provide full administrative rights to the system.

SYSTEMS AFFECTED:

Cisco UCS Director Software versions prior to Cisco UCS Director Release 4.0.0.3 HOTFIX

RISK:

Government:

Large and medium government entities: **High**
Small government entities: **High**

Businesses:

Large and medium business entities: **High**
Small business entities: **High**

Home users: N/A

DESCRIPTION:

Cisco UCS Director (formerly Cisco Cloupia) delivers unified converged infrastructure management for administering computing, network, virtualization, and storage solutions based on Cisco UCS and Cisco Nexus solutions, or multivendor infrastructures from one self-service web interface.

A vulnerability in Cisco Unified Computing System (UCS) Director could allow an unauthenticated, remote attacker to take complete control of the affected device.

The vulnerability is due to a default root user account created during installation. An attacker could exploit this vulnerability by accessing the server command-line interface (CLI) remotely using the default account credentials. An exploit could allow the attacker to log in with the default credentials, which provide full administrative rights to the system.

The Cisco UCS Director CLI can be accessed via Secure Shell (SSH).

RECOMMENDATIONS:

The following actions should be taken:

Upgrade vulnerable Cisco products immediately after appropriate testing.

REFERENCES:

CISCO:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140219-ucsd

https://tools.cisco.com/bugsearch/bug/CSCui73930